CLAIMS

1. A computing environment, comprising:

an operating system;

a virtual machine operating on said operating system;

a first application operating on said virtual machine;

a second application operating on said virtual machine; and

a first firewall control block, wherein said first firewall control block defines access privileges of said first application with respect to said second application, and further defines the access privileges of said second application with respect to said first application.

2. A computing environment as recited in claim 1, wherein said computing environment further comprises:

a second firewall control block, wherein said second firewall control block defines access privileges of said second application with respect to said first application, and further defines the access privileges of said first application with respect to said first application.

3. A computing environment as recited in claim 1, wherein said first firewall control block defines access privileges of said first application with respect to any other application in said computing environment, and further defines the access privileges of said any other application with respect to said first application.

4. A computing environment as recited in claim 3, wherein said first firewall control block includes a firewall control value and a firewall control indicator.

5. A computing environment as recited in claim 4,

wherein said firewall control value is a access privileges control value represented by one or more bytes, and

wherein said firewall control value is an indicator value represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of other applications.

6. A computing environment as recited in claim 4,

wherein said computing environment is a Java™ compliant computing environment,

wherein said first and second applications are Java™ compliant applets, and

wherein said first firewall control value includes a RID.

7. A computing environment as recited in claim 4,

wherein said computing environment is a Java™ compliant computing environment, and

wherein said first and second applications are Java™ compliant applets,

wherein said first firewall control block includes an AID.

8. A computing environment as recited in claim 4, wherein said computing environment is a Java™ card compliant computing environment, and,

wherein said first firewall control block is implemented as in the run rime environment.

9. A mobile computing device, comprising:

an operating system;

a Java™ compliant virtual machine operating on said operating system;

a first Java™ compliant applet operating on said Java™ compliant virtual machine;

a Java™ compliant applet operating on said virtual machine Java™ compliant virtual machine; and

a first firewall control block, wherein said first firewall control block defines access privileges of said first Java™ compliant applet with respect to at least one other Java™ compliant applet operating on said Java™ compliant virtual machine, and further defines the access privileges of said at least one other Java™ compliant applet Java™ compliant applet with respect to said first Java™ compliant applet.

10. A mobile computing device as recited in claim 9, wherein said mobile device is a Java™ compliant smart card.

11. A mobile computing device as recited in claim 10, wherein said first firewall control block includes a firewall control value and a firewall control indicator.

12. A mobile computing device as recited in claim 10,

wherein said firewall control value is a access privileges control value represented by one or more bytes, and

wherein said firewall control value is an indicator value represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of other applications.

13. A mobile computing device as recited in claim 10, wherein said first firewall control block includes a RID.

14. A mobile computing device as recited in claim 10, wherein said first firewall control block includes a PID.

15. A mobile computing device as recited in claim 10, wherein for a firewall control block is defined for every Java™ compliant applet

16. A method of providing security for a Java™ compliant computing environment that includes a Java™ virtual machine and a plurality of Java™ compliant applets that operate on said Java™ virtual machine, said method comprising:

receiving a request from a first Java™ compliant applet operating on Java™ virtual machine to access a second Java™ compliant applet;

reading a firewall control block associated with said second Java™ compliant applet;

determining, based on said firewall control block, whether said first Java™ compliant applet should be allowed to access said second Java™ compliant applet; and

allowing said first Java™ compliant applet to access said second Java™ compliant applet when said determining determines that access should be allowed.

17. A method as recited in claim 16, wherein said method further comprises:

providing a reference to said first Java™ compliant applet with a reference to said second Java™ compliant when said determining determines that access should be allowed.

18. A method as recited in claim 16, wherein said providing of a reference comprises:

invoking a first method implemented that is implemented as a part of Java™ management (or system) environment; and

invoking a second method that is implemented as a Applet class, as a result of said invoking of the second method,

19. A method as recited in claim 16, wherein said determining of whether said first Java™ compliant applet should be allowed to access said second Java™ compliant applet comprises:

reading a firewall control value; and

reading a firewall control indicator.

20. A method as recited in claim 16, wherein said determining of whether said first Java™ compliant applet should be allowed to access said second Java™ compliant applet comprises:

reading a first PID associated with said first Java™ compliant applet;

reading a second PID associated with said second Java™ compliant applet;

determining whether said first PID matches said second PID; and

allowing access only when said determining determines that said first PID matches said second PID.

21. A method as recited in claim 16, wherein said determining of whether said first Java™ compliant applet should be allowed to access said second Java™ compliant applet comprises:

reading a first AID associated with said first Java™ compliant applet;

reading a second AID associated with said second Java™ compliant applet;

determining whether said first AID matches said second AID; and

allowing access only when said determining determines that said first AID matches said second AID

22. A computer readable media including computer program code for providing security for a computing environment, said computer readable media comprising:

computer program code for receiving a request from a first application to access a second application;

computer program code for reading a firewall control block associated with said second application;

determining, based on said firewall control block, whether said first application should be allowed to access said second application; and

allowing said first application to access said second application when said determining determines that access should be allowed.